SIMULTANEOUS RATIONAL APPROXIMATIONS OF p-ADIC NUMBERS BY THE LLL LATTICE BASIS REDUCTION ALGORITHM (Nonlinear Analysis and Convex Analysis)

AUTHOR(S):

井上, 裕仁; 内藤, 幸一郎

数理解析研究所講究録
第1923巻 2014年 163-171

SIMULTANEOUS RATIONAL APPROXIMATIONS OF p-ADIC NUMBERS BY THE LLL LATTICE BASIS REDUCTION ALGORITHM

HIROHITO INOUE AND KOICHIRO NAITO

DEPARTMENT OF APPLIED MATHEMATICS, GRADUATE SCHOOL OF SCIENCE AND TECHNOLOGY, KUMAMOTO UNIVERSITY

1. Introduction

In this paper we construct multi-dimensional p-adic approximation lattices by simultaneous rational approximations of p-adic numbers. For analyzing these p-adic lattices we apply the LLL algorithm due to Lenstra, Lenstra and Lovász, which has been widely used to solve the various NP problems such as SVP (Shortest Vector Problems), ILP (Integer Linear Programing) .. and so on. In a two-dimensional lattice the Gauss reduction algorithm for finding the shortest vector is most powerful and useful. The LLL algorithm, which is a multi-dimensional extension of the Gauss algorithm, approximately solves SVP within a factor of $2^{O(n)}$ for the lattice dimension $n(\geq 3)$ in polynomial times.

Using the open source software SAGE, we compare the minimum norms of the vectors given by the LLL reduction algorithm and the norms of vectors estimated by the simultaneous approximation theory. We also study the two types of simultaneous approximations of p-adic numbers, which can be transferred from one of types to the other type by the famous Transference Principle. The Transference Principle only gives the equivalence relation between these two types on the existence of solutions of approximation inequalities. Any algorithms, which give the constructive relations between these two types of solutions, have not yet been known. Here we can give this algorithm by using LLL reduction algorithms.

2. Lattice and LLL algorithm

In this section we give a brief review on lattices and the LLL algorithm. (For details, see [4], [5].)

Given linearly independent vectors $b_1, ..., b_n \in \mathbb{R}^m$, the lattice generated by these vectors is defined by

$$L(b_1, ..., b_n) = \{\sum_{i=1}^{n} x_i b_i : x_i \in \mathbb{Z}\}.$$

We refer to $b_1, ..., b_n$ as a basis of the lattice.

2010 *Mathematics Subject Classification.* 11E95, 11A05, 11A55.
Key words and phrases. P-adic theory, Continued fractions, LLL algorithm.

Let B be the $m \times n$ matrix whose columns are $b_1, ..., b_n$, then the lattice generated by B is

$$L(B) = \{Bx : \ x \in \mathbb{Z}^n\}.$$

We say that the rank of lattice is n and its dimension is m. If $n = m$, the lattice is called a full-rank lattice. Hereafter we consider full-rank lattices.

For matrix B, $P(B) = \{Bx : x \in [0,1)^n\}$ is called the fundamental parallelepiped of B. Let $\Lambda = L(B)$ be a lattice of rank n. We define the determinant of Λ, denoted by $\det(\Lambda)$, as the n-dimensional volume of $P(B)$. In the full rank case, $\det(\Lambda) = |\det(B)|$.

The ith successive minimum of lattice Λ, $\lambda_i(\Lambda)$, is defined by

$$\lambda_i(\Lambda) = \inf\{r : \ \dim(span(\Lambda \cap \overline{B}(0,r))) \geq i\}.$$

The length of the shortest nonzero vector in the lattice is denoted by $\lambda_1(\Lambda)$ and the second minimum vector should be linearly independent to the shortest vector. The following estimate for the shortest vector is given by Minkowski's theorem.

$$\lambda_1(\Lambda) \leq \sqrt{n}\{\det(\Lambda)\}^{1/n}. \tag{2.1}$$

Next we introduce the algorithm given by Lenstra, Lenstra and Lovász, which approximately solves the Shortest Vector Problem (SVP) within a factor of $2^{O(n)}$ for the lattices dimension n. The basic idea of LLL algorithm is to generalize Gauss's algorithm to higher dimensions. For a basis $b_1, ..., b_n$ of a lattice, the Gram-Schmidt orthogonalized basis $b_1^*, ..., b_n^*$, which satisfies

$$span(b_1, ..., b_k) = span(b_1^*, ..., b_k^*), k = 1, ..., n$$

$$b_k = \sum_{i=1}^{k} \mu_{k,i} b_i^*, \ \mu_{k,i} = \frac{(b_k, b_i^*)}{(b_i^*, b_i^*)} \text{ for } \ i \leq k-1, \ \mu_{k,k} = 1,$$

is essentially used to construct the reduced basis.

Definition 2.1. For a constant $\delta : 1/4 < \delta < 1$, a basis $\{b_1, ..., b_n\}$ of a lattice is called a δ-reduced basis if it satisfies the following two conditions.

- $|\mu_{k,i}| = \left|\frac{(b_k, b_i^*)}{(b_i^*, b_i^*)}\right| \leq \frac{1}{2}$ for all $i < k$,
- for any pair of consecutive vectors b_i, b_{i+1},

$$\delta \|\pi_i(b_i)\|^2 \leq \|\pi_i(b_{i+1})\|^2$$

where we define projection operations π_i from $\mathbb{R}^n$ onto $span(b_i^*, b_{i+1}^*, ..., b_n^*)$ by

$$\pi_i(x) = \sum_{j=i}^{n} \frac{(x, b_j^*)}{(b_j^*, b_j^*)} b_j^*.$$

The following estimate is well-known for the first vector in a δ-LLL reduced basis.

Lemma 2.2. *If $B = (b_1, ..., b_n) \in \mathbb{R}^{n \times n}$ is a δ-LLL reduced basis with $\delta \in (1/4, 1)$, then*

$$\|b_1\| \leq \left(\frac{2}{\sqrt{4\delta - 1}}\right)^{n-1} \lambda_1(B). \tag{2.2}$$

Using the estimate (2.1), we obtain

$$\|b_1\| \leq \sqrt{n}\ |\det(B)|^{\frac{1}{n}} \left(\frac{2}{\sqrt{4\delta - 1}}\right)^{n-1}. \tag{2.3}$$

3. p-ADIC LATTICE

In this section we introduce p-adic approximation lattices and investigate simultaneous rational approximations of p-adic numbers. Let p be a fixed rational prime number and $|\cdot|_p$ be the corresponding p-adic valuation, normalized so that $|p|_p = p^{-1}$. The completion of $\mathbb{Q}$ w.r.t. $|\cdot|_p$ is called the field of p-adic numbers, denoted by $\mathbb{Q}_p$. The strong triangle inequality

$$|a + b|_p \leq \max\{|a|_p, |b|_p\}, \quad a, b \in \mathbb{Q}_p$$

is most important and essential to construct p-adic approximation lattices. The set of p-adic integers is defined by $\mathbb{Z}_p = \{z \in \mathbb{Q}_p : |z|_p \leq 1\}$.

Let $n \geq 1$ be an integer and let $\Xi = \{\xi_1, \xi_2, ..., \xi_n\}$ be a n-tuple of p-adic integers.

Definition 3.1. We denote by $w_n(\Xi)$ the supremum of the real numbers w such that, for some infinitely many real numbers X_j, which goes to infinity, the inequalities

$$0 < |a_{0,j} + a_{1,j}\xi_1 + \cdots + a_{n,j}\xi_n|_p \leq X_j^{-w-1},$$
$$\max_{0 \leq i \leq n} |a_{i,j}| \leq X_j,$$

have a solution in integers $a_{0,j}, a_{1,j}, ..., a_{n,j}$.

It follows from the Dirichlet principle that $w_n(\Xi) \geq n$ holds for every n-tuple Ξ of p-adic numbers.

For a positive integer m we define the p-adic approximation lattice Γ_m by

$$\Gamma_m = \{(a_0, a_1, ..., a_n) \in \mathbb{Z}^{n+1} : |a_0 + a_1\xi_1 + \cdots + a_n\xi_n|_p \leq p^{-m}\}.$$

When a p-adic integer ξ_i has the p-adic expansion

$$\xi_i = \sum_{k=0}^{\infty} x_{i,k}p^k, \ 0 \leq x_{i,k} \leq p - 1,$$

let $\xi_{i,m}$ be the m-th order approximation of ξ_i defined by

$$\xi_{i,m} = \sum_{k=0}^{m-1} x_{i,k}p^k.$$

Consider the basis $\{b_{0,m}, b_{1,m}, ..., b_{n,m}\} \subset \mathbb{Z}^{n+1}$ of the lattice Γ_m given by

$$b_{0,m} = (p^m, 0, ..., 0)^t, \quad b_{1,m} = (\xi_{1,m}, -1, 0, ..., 0)^t,$$
$$b_{2,m} = (\xi_{2,m}, 0, -1, 0, ..., 0)^t, \cdots, b_{n,m} = (\xi_{n,m}, 0, ..., 0, -1)^t.$$

In fact, we have $b_{k,m} \in \Gamma_m$, $\forall k$, since we can estimate

$$|\xi_{k,m} - \xi_k|_p \leq p^{-m}.$$

For $B_m = (b_{0,m} b_{1,m} ... b_{n,m})$ we have

$$B_m = \begin{pmatrix} p^m & \xi_{1,m} & \xi_{2,m} & \dots & \xi_{n,m} \\ 0 & -1 & 0 & \dots & 0 \\ 0 & 0 & -1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & -1 \end{pmatrix}, \quad |\det(B_m)| = p^m.$$

Applying the LLL algorithm for $\delta \in (1/4, 1)$, we denote $\{b_0, b_1, ..., b_n\}$ a reduced basis and $B = (b_0\ b_1\ ...\ b_n)$. It follows from (2.3) that the shortest vector b_0 in B satisfies

$$\begin{aligned} (3.1) \qquad \|b_0\| &\le \sqrt{n+1}\ |\det(B)|^{\frac{1}{n+1}} \left(\frac{2}{\sqrt{4\delta - 1}}\right)^n \\ &= \sqrt{n+1}\ |\det(B_m)|^{\frac{1}{n+1}} \left(\frac{2}{\sqrt{4\delta - 1}}\right)^n \\ &= \sqrt{n+1}\ p^{\frac{m}{n+1}} \left(\frac{2}{\sqrt{4\delta - 1}}\right)^n. \end{aligned}$$

Furthermore, it is known that

$$\left(\prod_{i=0}^{n} \|b_i\|\right)^{\frac{1}{n+1}} \le K_n |\det(B)|^{\frac{1}{n+1}} = K_n p^{\frac{m}{n+1}}, \quad K_n \sim 2^{O(n)}$$

for the reduced basis $\{b_0, b_1, ..., b_n\}$.

On the other hand, since for $\Xi = \{\xi_1, ..., \xi_n\}$ the inequality $w_n(\Xi) \ge n$ holds, we have the sequence $\{X_m\}$, going to infinity, and the sequence of integers $a_{0,m}, a_{1,m}, ..., a_{n,m}$, which satisfy the following inequalities

$$\begin{aligned} (3.2) \qquad & 0 < |a_{0,m} + a_{1,m}\xi_1 + \cdots + a_{n,m}\xi_n|_p \le X_m^{-n-1}, \\ & \max_{0 \le i \le n} |a_{i,m}| \le X_m, \quad \forall m. \end{aligned}$$

Thus, putting $X_m^{-n-1} = p^{-m}$, that is, $X_m = p^{\frac{m}{n+1}}$, we can admit that the LLL algorithm gives the approximate solutions of the simultaneous approximation problem (3.2). In section 5 we give the numerical calculations, comparing these two solutions.

4. Transference Theorem

We consider the following type of simultaneous approximation problems.

Definition 4.1. We denote by $\lambda_n(\Xi)$ the supremum of the real numbers λ such that, for some infinitely many real numbers Y_m, which goes to infinity, the inequalities

$$\begin{aligned} & 0 < \max_{1 \le i \le n} |a_{0,m}\xi_i - a_{i,m}|_p \le Y_m^{-\lambda-1}, \\ & \max_{0 \le i \le n} |a_{i,m}| \le Y_m, \end{aligned}$$

have a solution in integers $a_{0,m}, a_{1,m}, ..., a_{n,m}$.

Applying Khintchine's transference principle ([2], [3], for p-adic case see [7]), it is known that the following inequality relations between the two types of p-adic simultaneous approximations hold.

$$\frac{1}{n} \leq \frac{w_n(\Xi)}{(n-1)w_n(\Xi)+n} \leq \lambda_n(\Xi) \leq \frac{w_n(\Xi)-n+1}{n}. \tag{4.1}$$

The famous transference principle implies the equivalence of the inequalities between the 1st approximation problem given by Definition 3.1 and the 2nd approximation problem given by Definition 4.1 . Next we construct the algorithm, which gives the solutions of the 2nd approximation problem from the solutions of the 1st approximation problem by using the LLL algorithm.

For p-adic integers $\{\xi_1, ..., \xi_n\}$ and their m-th order approximations $\{\xi_{1,m}, ..., \xi_{n,m}\}$, let

$$B_m = \begin{pmatrix} p^m & \xi_{1,m} & \xi_{2,m} & \cdots & \xi_{n,m} \\ 0 & -1 & 0 & \cdots & 0 \\ 0 & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -1 \end{pmatrix}.$$

Applying the LLL reduction to the lattice $L(B_m)$, we can get the LLL reduced basis $\{b_0, b_1, ..., b_n\}$ and we can obtain the matrix $B = (b_0\ b_1 \cdots b_n)$.

Define the change of basis matrix D by

$$D = B(B_m)^{-1}.$$

Next, considering the transpose of B_m, define the matrix D' by

$$D' = (B_m^T)^{-1}B$$

and put $D'' = |\det(B_m)|D'$. We denote the first column of the matrix D'' by

$$(Q_m\ P_{1,m}\ P_{2,m} \cdots P_{n,m})^T.$$

Theorem 4.2. *The tuple of integers $\{Q_m, P_{1,m}, P_{2,m}, \cdots, P_{n,m}\}$ is a solution of the following 2nd-type simultaneous approximation problem*

$$|P_{i,m} - Q_m\xi_i|_p \leq p^{-m}, \forall i = 1, ..., n,$$
$$\max_{1\leq i\leq n}\{|P_{i,m}|\} \leq K_n p^{m(1+\frac{1}{n+1})},\quad |Q_m| \leq K_n p^{\frac{m}{n+1}},\ K_n \sim 2^{O(n)}.$$

except the following rare case where for some ξ_k

$$|P_{k,m} - Q_m\xi_{k,m}|_p > p^{-m} \text{ and} \tag{4.2}$$
$$(P_{k,m} - Q_m\xi_{k,m})\xi_k + \sum_{i\neq k}(P_{i,m} - Q_m\xi_{i,m})\xi_i \equiv 0 \mod p^m. \tag{4.3}$$

Remark 4.3. When we randomly choose a p-adic integer ξ, the probability of satisfying the relation $\xi \equiv 0 \mod p^m$ is p^{-m}.

5. Numerical calculations by LLL

Using the open source software SAGE, we compare the minimum and maximum norms of the vectors given by the LLL reduction algorithm and the norms of vectors estimated by the simultaneous approximation theory, using $X_m = p^{m/(n+1)}$. We investigate the following case.

- $p = 13$: prime number
- $\xi_i = a_i^{\frac{1}{103}}$: p-adic number, 103rd root of a_i
  $a_i = 3, 5, 9, 12, 29, 31, 41, 50, 53, 61, 75, 83, 89, 92, 96,$
  $101, 109, 123, 140, 154, 164, 167, 172, 175, 185, 196,$
  $200, 203, 214, 222, 229, 235, 254, 267, 276, 288, 298,$
  $300, 307, 313, 337, 340, 352, 363, 370, 375, 389, 396,$
  $404, 410, 418, 425, 437, 441, 446, 453, 478, 485, 492, 498$
- $m = 5, 6, ..., 40$: approximation orders
- $n = 10, 20, 60$: dimensions

First we show our numerical process by using the small parameters, $n = 10$, $\xi_i = a_i^{\frac{1}{103}}$, $m = 5$. For the approximation order $m = 5$ and the dimension $n = 10$, we operate the LLL reduction ($\delta = 0.99999$). Then we obtain the reduced basis B from B_m. Here we note that the basis is given by row vectors in SAGE.

$$B_m = \begin{pmatrix}
371293 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
352823 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
248971 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
293926 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
286272 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
267283 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
317273 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\
89958 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
227177 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\
144444 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\
57443 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1
\end{pmatrix}$$

$$B = \begin{pmatrix}
1 & -1 & -2 & 0 & 0 & 0 & -1 & -1 & -1 & 0 & 0 \\
1 & 1 & 2 & -1 & -1 & -1 & 0 & -1 & -1 & 0 & -1 \\
0 & 1 & 0 & -1 & 0 & -2 & 0 & -2 & 0 & -1 & 1 \\
1 & -1 & -1 & 0 & 0 & 1 & 0 & -1 & 1 & -2 & 2 \\
0 & 1 & 1 & 0 & 3 & -1 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 0 & -3 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 1 & 1 & 1 & -2 & -1 & -2 & -2 & 0 \\
0 & -1 & 1 & 0 & -2 & -1 & -1 & 1 & -1 & -1 & 1 \\
0 & -2 & 0 & 0 & 2 & -1 & -1 & 1 & 0 & 0 & -2 \\
0 & 0 & -1 & 3 & 1 & 0 & 1 & -2 & 0 & 0 & 1 \\
-2 & -2 & 2 & -2 & -1 & 0 & 1 & -2 & 0 & 1 & 1
\end{pmatrix}$$

We obtain

$$\|b_1\| = 3, \ \|b_{n+1}\| = 4.898979...,$$

which are sufficiently effective solutions of SVP, comparing to the theoretical value

$$X_m = p^{m/(n+1)} = 3.208764....$$

Next we give the graphs which compare these numerical values for the SVP by LLL and the theoretical values X_m for the approximation orders m from 5 to

40 and the dimensions $n = 10, 20, 60$. The following graphs show that the LLL algorithm is strong enough to solve the SVP of dimensions under 100.

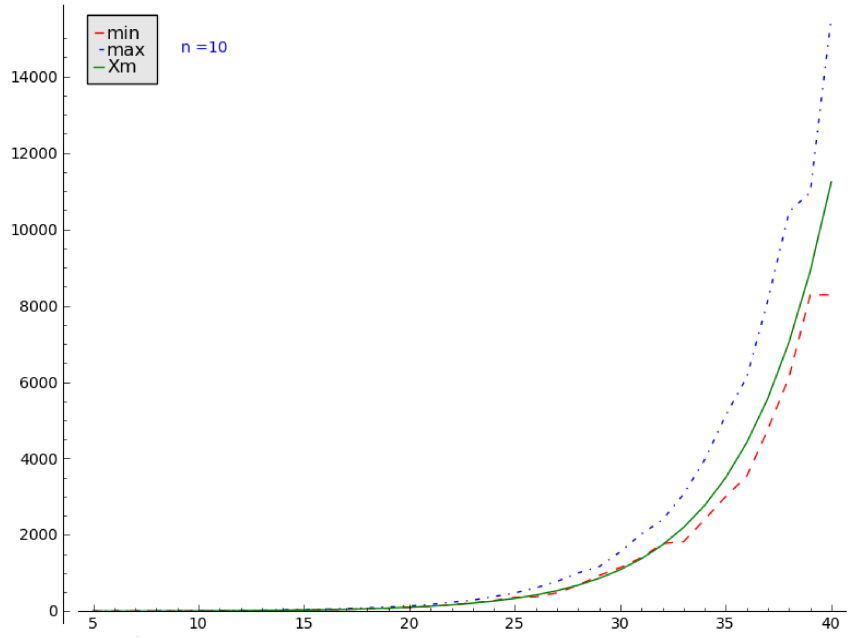

FIGURE 1. n=10

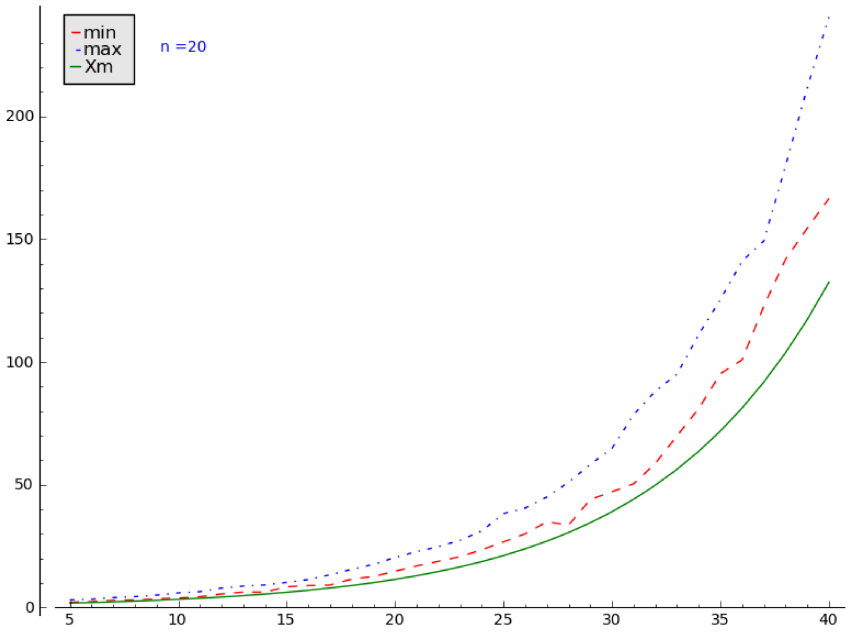

FIGURE 2. n=20

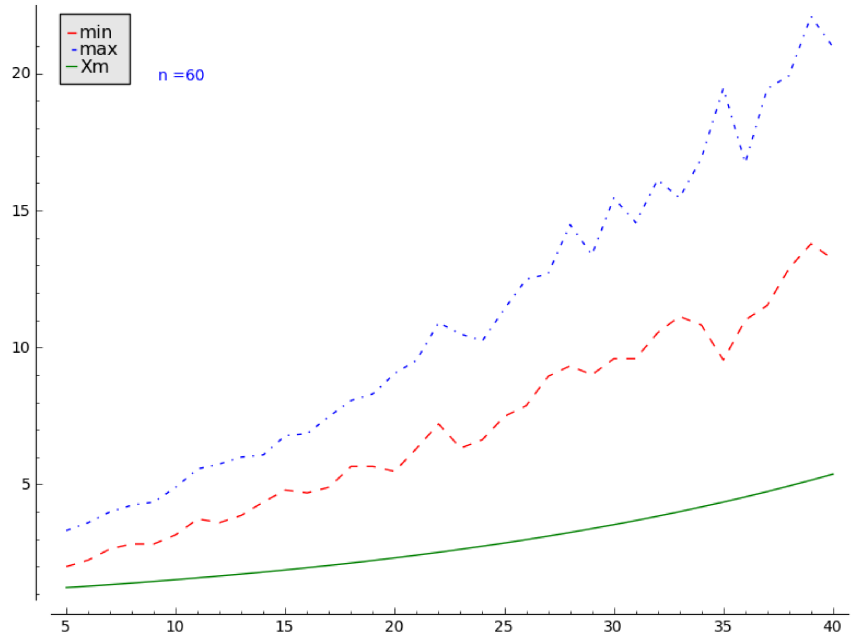

FIGURE 3. n=60

6. NUMERICAL CALCULATIONS FOR TRANSFERENCE PRINCIPLE

We apply the algorithm given in section 4 to obtain the solutions of the 2nd type simultaneous approximation problem for the parameters $p = 13, n = 4, m = 10, \xi_i = a_i^{\frac{1}{103}}, a_i = 5, 29, 53, 61$.

$$B_m = \begin{pmatrix} 137858491849 & 0 & 0 & 0 & 0 \\ 76365194160 & -1 & 0 & 0 & 0 \\ 51552443868 & 0 & -1 & 0 & 0 \\ 66523226082 & 0 & 0 & -1 & 0 \\ 72516179394 & 0 & 0 & 0 & -1 \end{pmatrix}.$$

Applying the LLL algorithm to B_m, we obtain the LLL reduced matrix B.

$$B = \begin{pmatrix} -56 & 11 & 12 & 78 & 30 \\ -23 & 22 & -50 & -62 & 151 \\ -98 & 80 & -22 & -96 & -87 \\ -14 & -149 & 105 & -29 & -9 \\ 20 & 138 & 234 & -25 & -34 \end{pmatrix}$$

Since $p^{m/(n+1)} = 169$, almost all elements of B is less than $p^{m/(n+1)}$.
We can obtain the change of basis matrix D by

$$D = B(B_m)^{-1} = \begin{pmatrix} 64 & -11 & -12 & -78 & -30 \\ 43 & -22 & 50 & 62 & -151 \\ -56 & -80 & 22 & 96 & 87 \\ -62 & 149 & -105 & 29 & 9 \\ 134 & -138 & -234 & 25 & 34 \end{pmatrix}.$$

We give the 2nd-type simultaneous approximations, using the matrix D' defined by $D' = B(B_m^T)^{-1}$.

$$|\det(B_m^T)|D' = |\det(B_m^T)|B(B_m^T)^{-1}$$

$$= \begin{pmatrix} -56 & -5792894283299 & -4541238758796 & -14478263024814 & -8196660801534 \\ -23 & -4789286286358 & 5707218383486 & 7017192294752 & -22484504395261 \\ -98 & -18512468375600 & -2019252678386 & 6715139061468 & 4887103210251 \\ -14 & 19471802567261 & -15196875858297 & 3066571098473 & 225499915125 \\ 20 & -17497167991962 & -31227838215306 & 4776926817865 & 6137512310746 \end{pmatrix}$$

We denote the first row of this matrix by

$$\begin{pmatrix} Q & P_1 & P_2 & \cdots & P_n \end{pmatrix}.$$

Then we can calculate

i	1	2	3	4
$\lvert P_i - Q\xi_i\rvert_p$	13^{-10}	13^{-11}	13^{-10}	13^{-10}

Since $p^{-m} = 13^{-10}$, we obtain the following 2nd-type simultaneous approximations

$$|P_i - Q\xi_i|_p \leq p^{-m}, \forall i = 1, ..., n.$$

References

1. Y.Bugeaud, "Approximation by Algebraic Numbers", Cambridge Tracts in Mathematics, Cambridge University Press, 2004.
2. J.W.S.Cassels, "An introduction to Diophantine approximation", Cambridge Tract 45, Cambridge Univ. Press, 1957
3. Y.A.Khinchin, "Continued Fractions", the University of Chicago Press 1964. 28 # 5037
4. D. Micciano and S. Goldwasser, "Complexity of Lattice Problems, a Cryptographic Perspective", Springer International Series in Engineering and Computer Science, vol. 671. Springer, 2002
5. P.Q. Nguyen and B. Vallee (Eds.), "The LLL Algorithm, Survey and Applications", Springer 2010.
6. W.M.Schmidt, "Diophantine Approximation", Springer Lecture Notes in Math. 785, 1980.
7. V.G. Sprindžuk, Mahler's problem in metric number theory. Izdat. "Nauka i Tehnika", Minsk, 1967 (in Russian). English translation by B. Volkmann, Translations of Mathematical Monographs, Vol. 25, American Mathematical Society, Providence, R.I., 1969

Department of Applied Mathematics,
Graduate School of Science and Technology,
Kumamoto University,
Kurokami 2-39-1, Kumamoto, Japan
132d9307@st.kumamoto-u.ac.jp
knaito@gpo.kumamoto-u.ac.jp

熊本大学大学院・自然科学研究科　井上 裕仁
熊本大学大学院・自然科学研究科　内藤 幸一郎